CLAIMS

What is claimed is:

1. A method for secure computer communications, comprising:

generating a Rivest-Shamir-Adleman ("RSA") algorithm public / private key pair at a web server, wherein <N, e'>, represents the public key with N being the product of two distinct primes, p and q, and wherein the private key is represented by d;

sending a client hello message to the web server from a client requesting a secure network connection;

responding to the client with a server hello message comprising the RSA public key;

encrypting a random string R at the client using the RSA public key, wherein the resulting cipher-text C includes R;

sending the encrypted cipher-text to the web server;

decrypting the cipher-text at the web server using the RSA private key wherein $d=r_1 \bmod (p-1)$ and $d=r_2 \bmod (q-1)$, and wherein $<r_1, r_2>$ are relatively small numbers on the order of 160 bits in length, wherein R'_1 equals the cipher-text raised to the r_1 power moduli one of the distinct prime numbers and R'_2 equals the cipher-text raised to the r_2 power moduli the remaining prime number;

combining R'_1 and R'_2 to produce R using the Chinese Remainder Theorem wherein finding R'_1 and R'_2 is more efficient than using standard RSA keys; and

establishing a common session key between the web server and client using R.

2. The method of claim 1, wherein the secure communications includes Secure Socket Layer ("SSL") messages.

3. The method of claim 1, wherein the secure communications includes Transport Layer Security ("TLS") messages.

4. The method of claim 1, wherein the secure communications includes internet protocol secure ("IPSec") messages.

5. The method of claim 1, wherein generating a RSA public / private key pair includes;

taking the product of the n-bit primes to produce an arbitrary number N;

picking two random k-bit values r_1 and r_2 such that r_1 and r_2 are on the order of 160 bits and are mathematically related to the n-bit primes and e' is related to N; and

sending the public key to a certificate authority and receiving back from the certificate authority a public key certificate for a public key wherein e' is on the order of N in size.

6. The method of claim 5, wherein the k-bit values are related to the n-bit primes by the equations $\gcd(r_1, p-1) = 1$, $\gcd(r_2, q-1) = 1$, and $r_1 = r_2$

mod w, respectively, wherein gcd represents the greatest common divisor and w = gcd(p-1,q-1).

7. The method of claim 6, wherein the relationship between e' and N is expressed by the equation $e' = d^{-1} \bmod \varphi(N)$.

8. The method of claim 1, wherein decrypting includes:

computing R_1' and R_2' as expressed by the relationship $R_1 = C^{r_1} \bmod p$ and $R_2 = C^{r_2} \bmod q$; and

applying the Chinese Remainder Theorem to produce R, wherein $R = R_1' \bmod p$ and $R = R_2' \bmod q$

9. A method for performing an initial handshake during secure communications in a computer network comprising:

coupling a client to a web server;

generating a Rivest-Shamir-Adleman ("RSA") algorithm public / private key pair at the web server, wherein the RSA public key is a product of two distinct prime numbers and the private key is a function of two random numbers, wherein each random number has a number of bits greater than or equal to 160 bits and less than a number of bits of the RSA key;

sending a client hello message to the web server requesting a secure network connection;

responding to the client with a server hello message containing the RSA

public key;

encrypting a random string R at the client using the RSA public key, wherein the resulting cipher-text C includes R;

sending the encrypted cipher-text message to the web server;

separating cipher-text moduli of the two distinct prime numbers;

decrypting the moduli of the two distinct prime numbers individually using the two random numbers, wherein the results are combined using the Chinese Remainder Theorem, wherein computational efficiency is improved; and

establishing a common session key between the web server and the client using R.

10. The method of claim 9, wherein the initial handshake of secure communications includes Secure Socket Layer ("SSL") messages.

11. The method of claim 9, wherein the initial handshake of secure communications includes Transport Layer Security ("TLS") messages.

12. The method of claim 9, wherein the initial handshake of secure communications includes internet protocol secure ("IPSec") messages.

13. The method of claim 9, further comprising:

combining individually encrypted messages into a set of encrypted messages wherein each encrypted message possesses a public key comprising

an encryption exponent;

determining a root node of a binary tree containing leaf nodes corresponding to each encryption exponent using a plurality of separate parallel batch trees, wherein the root node of each tree is found and combined to determine the final answer;

minimizing a disparity between sizes of the encryption exponents of the within the set;

using simultaneous multiple exponentiation such that the encryption exponents are combined to reduce the number of exponentiations;

calculating a product of the encrypted messages;

extracting at least one root from the product of the encrypted messages; and

decrypting the encrypted messages by expressing the at least one root as at least one promise and evaluating the at least one promise at the leaf nodes, and multiplying an inversion of a total product of the leaf nodes with a partial product of the leaf nodes forming an inversion of the leaf node, producing a reduced number of modular inversions wherein efficiency of the decryption is increased.

14. The method of claim 9, further comprising keeping the size of N constant while reducing the size of the two distinct prime numbers such that the size of the two distinct prime numbers is on the order of one third of the size of N.

15. A method for secure communications, comprising:

generating a Rivest-Shamir-Adleman ("RSA") algorithm public / private key pair at a web server, wherein the RSA public key is a product of two distinct prime numbers and the private key is a function of two random numbers;

receiving a client hello message from a client requesting a secure socket layer ("SSL") coupling;

responding to the client with a server hello message containing the RSA public key;

encrypting a random string R at the client using the RSA public key, wherein the resulting cipher-text includes R;

receiving the encrypted cipher-text message at the web server;

separating cipher-text moduli of the two distinct prime numbers;

decrypting the moduli of the distinct prime numbers individually using the two random numbers, wherein the results are combined using the Chinese Remainder Theorem; and

establishing a common session key between the web server and client using R.

16. A method for secure computer communications, comprising:

coupling a web server to a client wherein the client requests the formation of a secure network connection;

generating a Rivest-Shamir-Adleman("RSA") algorithm public / private key pair, the public key comprising a root N, wherein N of the RSA public key

is the product of two distinct n-bit prime numbers, p and q, wherein an encryption exponent e' of the RSA public key is of the same order in size as the public key root, N

encrypting a plain-text message R using the RSA public key such that the resulting text is cipher-text C;

decrypting the cipher-text C using the RSA private key wherein the RSA private key is a function of two roots r_1 and r_2, wherein the two roots each are on the order of 160 bits in length; and

using the plain-text message R to determine a session encryption key and a session integrity key.

17. A method for Rivest-Shamir-Adleman ("RSA") decryption of secure network communications, comprising:

generating a RSA public/private key pair at a web server, wherein <N, e> represents the public key that is mathematically related to two distinct prime numbers;

keeping a size of N constant while reducing a size of the two distinct prime numbers by calculating N from a product of a first distinct prime number raised to the first power and a second distinct prime number wherein the first power is greater than one;

using the public key by a client to encrypt a plain-text message R to form a cipher-text message C;

decrypting the cipher-text C at the web server by using the RSA private key d to determine the plain-text message R by finding R'_1 and R'_2, wherein the

private key is a function of two random numbers $<r_1 , r_2>$, and wherein an additional $R"_1$ is constructed by using one of the two distinct prime numbers raised to a power greater than one, wherein efficiency of the decryption is increased in response to the reduced size of the two distinct prime numbers; and

computing the plain-text message using the Chinese Remainder Theorem.

18. The method of claim 17, further comprising;

combining individually encrypted network security protection handshake messages into a set of encrypted messages wherein each encrypted message is derived using a public key containing an encryption exponent;

determining a root node of a binary tree comprising leaf nodes corresponding to each encrypted messages encryption exponent by using a plurality of separate, parallel batch trees finding the root node of each tree and combining the final answers;

minimizing the disparity between the sizes of the encryption exponents of the public keys within the set;

using simultaneous multiple exponentiation such that the encryption exponents are combined to reduce the number of exponentiations;

calculating a product of the encrypted messages;

extracting at least one root from the product of the encrypted messages; and

decrypting the encrypted messages by expressing the at least one root as at least one promise and evaluating the at least one promise at the leaf nodes,

and multiplying an inversion of a total product of the leaf nodes with a partial product of the leaf nodes forming an inversion of the leaf node wherein the decryption is increased by reducing the number of modular inversions.

19. The method of claim 17, wherein the k-bit values r_1, r_2 are related to the n-bit primes by the greatest common divisor of $(r_1, p-1) = 1$, $(r_2, q-1) = 1$, $r_1 = r_2 \bmod w$ respectively such that $d = r_1, \bmod p-1$, $d = r_2 \bmod q-1$, and w is equal to the greatest common divisor of $(p\text{-}1, q\text{-}1)$.

20. The method of claim 17, wherein decrypting includes:

computing R_1', R"$_1$, and R_2' as expressed by the relationships

$$R_1' = C^{r_1} \bmod p \ , \ R_2' = C^{r_2} \bmod q \text{ , and } R_1'' = R_1' - \frac{\left(R_1'\right)^e - C}{e\left(R_1'\right)^{e-1}} \left(\bmod p^2\right).$$

21. A method for generating a Rivest-Shamir-Adleman ("RSA") public / private key pair in secure network couplings, comprising:

generating two n-bit distinct prime numbers;

computing a public key root from a mathematical relationship between two distinct prime numbers;

reducing the size of the two distinct prime numbers while keeping the size of the public key root constant using exponentiation of the two distinct prime numbers;

forming a public RSA key pair by associating the public key root and a standard RSA encryption exponent; and

computing a private RSA key pair by mathematically combining the standard RSA encryption exponent and the n-bit distinct prime numbers.

22. The method of claim 21, wherein computing the public key root includes the product of the square of one n-bit prime number and the second n-bit prime number.

23. The method of claim 21, wherein the public RSA key pair is indistinguishable from a standard RSA pair.

24. The method of claim 21, further comprising:

encrypting a pre-master-secret using the public RSA key pair; and

decrypting the pre-master-secret using the private RSA key pair wherein Hensle lifting compensates for reducing the size of the distinct prime numbers.

25. A method for Rivest-Shamir-Adleman ("RSA") decryption of secure network communications, comprising:

generating a RSA public/private key pair at a web server, wherein <N, *e*> represents a public key that is mathematically related to two distinct prime numbers and d represents a private key that is mathematically related to two random numbers;

keeping a size of N constant while reducing a size of the two distinct prime number by calculating N from a product of a first distinct prime number raised to a power greater than one and the second distinct prime number;

using the public key at a client to encrypt a plain-text message R to form

a cipher-text message C;

decrypting the cipher-text C at the web server using the RSA private key d to determine the plain-text message R by finding R'_1 and R'_2, wherein an additional $R"_1$ is constructed by raising the first of the two distinct prime numbers to a power greater than one, wherein the efficiency of the decryption is increased due to a reduced size of the two distinct prime numbers using the private RSA key pair, wherein Hensle lifting compensates for altering a multiplicity of the distinct prime numbers; and

computing the plain-text message using the Chinese Remainder Theorem.

26. A method for Rivest-Shamir-Adleman ("RSA") decryption of secure network communications, comprising:

generating a RSA public/private key pair at the web server wherein <N, *e*> represents the public key that is mathematically related to two distinct prime numbers;

keeping a size of N constant while reducing a size of the two distinct prime numbers such that each of the two distinct prime numbers is on the order of one third of the size of N;

using the public key at a client to encrypt a plain-text message R to form a cipher-text message C;

decrypting the cipher-text C at the web server by using the RSA private key d, to determine the plain-text message R by finding R'_1 and R'_2, wherein an additional $R"_1$ is constructed by using the one of the two distinct prime numbers

raised to a power greater than one, wherein the efficiency of the decryption is increased in response to the reduced size of the two distinct prime numbers using the private RSA key pair wherein Hensle lifting compensates for altering the multiplicity of the distinct prime numbers; and

computing the plain-text message using the Chinese Remainder Theorem.

27. A system for Rivest-Shamir-Adleman ("RSA") decryption of secure network communications, comprising:

a web server generating a RSA public/private key pair wherein <N, *e*> represents a public key that is mathematically related to two distinct prime numbers;

the web server keeping a size of N constant while reducing a size of the two distinct prime numbers by calculating N from the product of a first distinct prime number raised to a power greater than one and a second distinct prime number;

a client using the public key to encrypt a plain-text message R to form a cipher-text message C;

the web server decrypting the cipher-text C by using the RSA private key d to determine the plain-text message R by finding R'_1 and R'_2, wherein an additional R''_1 is constructed by using one of the two distinct prime numbers raised to a power greater than one wherein the efficiency of the decryption is increased in response to the reduced size of the two distinct prime numbers; and

the web server computing the plain-text message using the Chinese Remainder Theorem.

28. A system for using Rivest-Shamir-Adleman ("RSA") decryption of secure network communications in a computer network, comprising:

at least one web server;

at least one client processor coupled to the at least one web server, wherein the at least one web server generates a RSA public/private key pair, <N, *e*>, representing the public key that is mathematically related to two distinct prime numbers, wherein d represents the private key;

the at least one web server keeping a size of N constant while reducing a size of the two distinct prime numbers by calculating N from the product of a first distinct prime number raised to a power greater than one and a second distinct prime number;

the at least one client processor using the public key to encrypt a plain-text message R to form a cipher-text message C;

the at least one web server decrypting the cipher-text message C by using the RSA private key $<r_1, r_2>$ to determine the plain-text message R by finding R'_1 and R'_2, wherein an additional R''_1 is constructed by using one of the two distinct prime numbers raised to a power greater than one wherein the efficiency of the decryption is increased in response to the reduced size of the two distinct prime numbers; and

the at least one web server computing the plain-text message using the Chinese Remainder Theorem.

29. A computer-readable medium, comprising executable instructions for Rivest-Shamir-Adleman ("RSA") decryption of secure network communications which, when executed in a processing system, causes the system to:

couple a web server to a client;

send a client hello message to the web server requesting a secure network connection;

generate a Rivest-Shamir-Adleman ("RSA") algorithm public / private key pair at the web server wherein the RSA public key is the product of two distinct prime numbers wherein the RSA private key is a function of two random numbers wherein each random number has a number of bits greater than or equal to 160 bits and less than a number of bits of the RSA key;

respond to the client with a server hello message containing the RSA public key;

encrypt a random string R at the client using the RSA public key, wherein the resulting cipher-text C includes R;

send the encrypted cipher-text message C to the web server;

separate cipher-text C moduli of the two distinct prime numbers;

decrypt the moduli of the two distinct prime numbers individually using the two random numbers, wherein results are combined using the Chinese Remainder Theorem, wherein computational efficiency is improved and

establish a common session key between the web server and the client using R.

30. An electromagnetic medium, comprising executable instructions for Rivest-Shamir-Adleman ("RSA") decryption of secure network communications which, when executed in a processing system, causes the system to:

couple a web server to a client;

send a client hello message to the web server requesting a secure network connection;

generate a Rivest-Shamir-Adleman ("RSA") algorithm public / private key pair at the web server wherein the RSA public key is the product of two distinct prime numbers, wherein the RSA private key is a function of two random numbers wherein each random number has a number of bits greater than or equal to 160 bits and less than a number of bits of the RSA key;

respond to the client with a server hello message containing the RSA public key;

encrypt a random string R at the client using the RSA public key, wherein the resulting cipher-text C includes R;

send the encrypted cipher-text message C to the web server;

separate cipher-text moduli of the two distinct prime numbers;

decrypt the moduli of the two distinct prime numbers individually using the two random numbers, wherein results are combined using the Chinese Remainder Theorem, wherein computational efficiency is improved; and

establish a common session key between the web server and the client using R.

31. A computer-readable medium, comprising executable instructions for Rivest-Shamir-Adleman ("RSA") decryption of secure network communications which, when executed in a processing system, causes the system to:

generate a RSA public/private key pair at the web server wherein <N, *e*> represents the public key that is mathematically related to two distinct prime numbers;

keep a size of N constant while reducing a size of the two distinct prime numbers such that each of the two distinct prime numbers is on the order of one third of the size of N;

use the public key at client to encrypt a plain-text message R to form a cipher-text message C;

decrypt the cipher-text C at the web server by using the RSA private key d to determine the plain-text message R by finding R'_1 and R'_2, wherein an additional R''_1 is constructed by using one of the two distinct prime numbers raised to a power greater than one, wherein the efficiency of the decryption is increased in response to the reduced size of the two distinct prime numbers using the private RSA key pair wherein Hensle lifting compensates for altering the multiplicity of the distinct prime numbers; and

compute the plain-text message using the Chinese Remainder Theorem.

32. An electromagnetic medium, comprising executable instructions for Rivest-Shamir-Adleman ("RSA") decryption of secure network

communications which, when executed in a processing system, causes the system to:

generate a RSA public/private key pair at the web server wherein <N, *e*> represents the public key that is mathematically related to two distinct prime numbers;

keep a size of N constant while reducing a size of the two distinct prime numbers such that each of the two distinct prime numbers is on the order of one third of the size of N;

use the public key at a client to encrypt a plain-text message R to form a cipher-text message C;

decrypt the cipher-text C at the web server by using the RSA private key d to determine the plain-text message R by finding R'_1 and R'_2, wherein an additional R''_1 is constructed by using one of the two distinct prime numbers raised to a power greater than one, wherein the efficiency of the decryption is increased in response to the reduced size of the two distinct prime numbers using the private RSA key pair wherein Hensle lifting compensates for altering the multiplicity of the distinct prime numbers; and

compute the plain-text message using the Chinese Remainder Theorem.